#2

IN THE U.S. PATENT AND TRADEMARK OFFICE

Applicant(s): MIYAGAWA, Akiko et al.

Application No.: Group:

Filed: November 26, 2001 Examiner:

For: ILLEGAL ACCESS DATA HANDLING APPARATUS AND METHOD FOR HANDLING ILLEGAL ACCESS DATA

L E T T E R

Assistant Commissioner for Patents
Box Patent Application
Washington, D.C. 20231

November 26, 2001
2565-0238P

Sir:

Under the provisions of 35 USC 119 and 37 CFR 1.55(a), the applicant hereby claims the right of priority based on the following application(s):

Country	Application No.	Filed
JAPAN	2001-036436	02/14/01

A certified copy of the above-noted application(s) is(are) attached hereto.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to deposit Account No. 02-2448 for any additional fees required under 37 C.F.R. 1.16 or under 37 C.F.R. 1.17; particularly, extension of time fees.

Respectfully submitted,

BIRCH, STEWART, KOLASCH & BIRCH, LLP

By: _____
MICHAEL K. MUTTER
Reg. No. 29,680
P. O. Box 747
Falls Church, Virginia 22040-0747

Attachment
(703) 205-8000
/sll

MIYAGAWA, Akiko et al.
November 26, 2001
BSKB, LLP
(703)205-8000
2565-0238P
1 of 1

日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００１年　２月１４日

出願番号
Application Number: 特願２００１－０３６４３６

出願人
Applicant(s): 三菱電機株式会社

２００１年　６月　４日

特許庁長官
Commissioner,
Japan Patent Office 及川耕造

出証番号　出証特２００１－３０５１８８２

【書類名】　特許願
【整理番号】　529273JP01
【提出日】　平成13年 2月14日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 13/00
【発明者】
　【住所又は居所】　東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
　【氏名】　宮川　明子
【発明者】
　【住所又は居所】　東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
　【氏名】　稲田　徹
【発明者】
　【住所又は居所】　東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
　【氏名】　後沢　忍
【特許出願人】
　【識別番号】　000006013
　【氏名又は名称】　三菱電機株式会社
【代理人】
　【識別番号】　100099461
　【弁理士】
　【氏名又は名称】　溝井　章司
【選任した代理人】
　【識別番号】　100111497
　【弁理士】
　【氏名又は名称】　波田　啓子

【選任した代理人】

【識別番号】　100111800

【弁理士】

【氏名又は名称】　竹内　三明

【手数料の表示】

【予納台帳番号】　056177

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9903016

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　不正侵入データ対策処理装置及び不正侵入データ対策処理方法

【特許請求の範囲】

【請求項１】　所定の内部通信ネットワーク外に配置され、

前記内部通信ネットワークに不正に侵入する目的で前記内部通信ネットワーク外に配置されたいずれかのデータ通信装置より送信された不正侵入データを受信し、受信した前記不正侵入データに対する対策処理を行うことを特徴とする不正侵入データ対策処理装置。

【請求項２】　前記不正侵入データ対策処理装置は、

前記内部通信ネットワーク内に配置されたデータ通信装置と前記内部通信ネットワーク外に配置されたデータ通信装置との間のデータ通信の中継を行うとともに前記不正侵入データを検知する不正侵入データ検知装置に接続され、

前記不正侵入データ検知装置より前記不正侵入データを受信することを特徴とする請求項１に記載の不正侵入データ対策処理装置。

【請求項３】　前記不正侵入データ対策処理装置は、

前記不正侵入データ検知装置より、前記不正侵入データを受信するデータ受信部と、

前記データ受信部により受信された前記不正侵入データを解析するデータ解析部と、

前記データ解析部による解析結果に基づき、前記不正侵入データに対する応答データを生成する応答データ生成部と、

前記応答データ生成部により生成された前記応答データを前記不正侵入データ検知装置に対して送信するデータ送信部とを有することを特徴とする請求項２に記載の不正侵入データ対策処理装置。

【請求項４】　前記データ受信部は、

前記不正侵入データ検知装置より、前記不正侵入データ検知装置によりカプセル処理された不正侵入データを受信し、

前記不正侵入データ対策処理装置は、更に、

前記データ受信部により受信されたカプセル処理された不正侵入データのカプ

セル処理を解除して不正侵入データを抽出するとともに、前記応答データに対してカプセル処理を行うカプセル処理部を有し、

前記データ送信部は、

前記カプセル処理部によりカプセル処理された応答データを前記不正侵入データ検知装置に対して送信することを特徴とする請求項３に記載の不正侵入データ対策処理装置。

【請求項５】　前記応答データ生成部は、

前記内部通信ネットワーク内に配置された特定のデータ通信装置が前記不正侵入データを受信した場合に、前記特定のデータ通信装置が前記不正侵入データに対して生成する応答データと同じ内容の応答データを生成することを特徴とする請求項３に記載の不正侵入データ対策処理装置。

【請求項６】　前記データ受信部は、

前記不正侵入データ検知装置より、前記不正侵入データ検知装置の通信履歴を示す通信履歴情報を受信し、

前記データ解析部は、

前記データ受信部により受信された前記通信履歴情報を解析し、前記通信履歴情報の解析結果に基づき前記内部通信ネットワーク外に配置された所定のデータ通信装置から送信されるデータを不正侵入データに指定する不正侵入データ指定情報を生成し、

前記データ送信部は、

前記データ解析部により生成された前記不正侵入データ指定情報を前記不正侵入データ検知装置に送信することを特徴とする請求項３に記載の不正侵入データ対策処理装置。

【請求項７】　前記データ受信部は、

前記不正侵入データ検知装置より、データ認証に用いる認証情報が添付された不正侵入データを受信し、

前記カプセル処理部は、前記認証情報を用いて前記不正侵入データのデータ認証を行うことを特徴とする請求項４に記載の不正侵入データ対策処理装置。

【請求項８】　前記カプセル処理部は、

前記応答データのデータ認証に用いる認証情報を前記応答データに添付し、

前記データ送信部は、

前記カプセル処理部により認証情報が添付された応答データを前記不正侵入データ検知装置に送信することを特徴とする請求項７に記載の不正侵入データ対策処理装置。

【請求項９】　所定の内部通信ネットワーク外において、

前記内部通信ネットワークに不正に侵入する目的で前記内部通信ネットワーク外に配置されたいずれかのデータ通信装置より送信された不正侵入データを受信し、受信した前記不正侵入データに対する対策処理を行うことを特徴とする不正侵入データ対策処理方法。

【請求項１０】　前記不正侵入データ対策処理方法は、

前記内部通信ネットワーク内に配置されたデータ通信装置と前記内部通信ネットワーク外に配置されたデータ通信装置との間のデータ通信の中継を行うとともに前記不正侵入データを検知する不正侵入データ検知装置と通信を行い、

前記不正侵入データ検知装置より前記不正侵入データを受信することを特徴とする請求項９に記載の不正侵入データ対策処理方法。

【請求項１１】　前記不正侵入データ対策処理方法は、

前記不正侵入データ検知装置より、前記不正侵入データを受信するデータ受信ステップと、

前記データ受信ステップにより受信された前記不正侵入データを解析するデータ解析ステップと、

前記データ解析ステップによる解析結果に基づき、前記不正侵入データに対する応答データを生成する応答データ生成ステップと、

前記応答データ生成ステップにより生成された前記応答データを前記不正侵入データ検知装置に対して送信するデータ送信ステップとを有することを特徴とする請求項１０に記載の不正侵入データ対策処理方法。

【請求項１２】　前記応答データ生成ステップは、

前記内部通信ネットワーク内に配置された特定のデータ通信装置が前記不正侵入データを受信した場合に、前記特定のデータ通信装置が前記不正侵入データに

対して生成する応答データと同じ内容の応答データを生成することを特徴とする請求項１０に記載の不正侵入データ対策処理方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

この発明は、コンピュータネットワークのセキュリティサポート契約者に対し、不正侵入を検知した契約者のネットワーク機器からの情報により、不正侵入者をおとりサーバに誘導する手段を提供する管理システムに関するものである。

【０００２】

【従来の技術】

従来のネットワークシステムでは、不正侵入検知機能を備えたネットワーク構成機器や管理装置によって、企業などの組織単位で独自にセキュリティ対策を施すのが主流であった。

例えば、特開２０００－９００３１によれば、ルータ間にネットワーク不正解析システムを設け、通信に不正を検出すると、通信当事者間の通信を傍受する方式、特開２０００－４７９８７では、不正アクセスを検知した場合、正規データベースとは別に用意した擬似データベースへの誘導を行い、正規データの流出を防ぐ方式、特開平６－６３４７では、セキュリティ管理装置を設け、不正アクセスを検知したネットワーク構成機器が管理装置に不正アクセス報告を通知し、管理装置にてセキュリティを集中管理する方式がある。

これらは、すべて企業などネットワークを運営する顧客がシステムを導入し、顧客自ら管理する方式である。

【０００３】

【発明が解決しようとする課題】

しかしながら、従来のネットワークシステムでは、組織の規模が小さい場合、ネットワーク管理者の確保や管理ノウハウの教育が難しいという問題があった。

また、専任のネットワーク管理者の確保が可能な場合でも、ネットワーク管理者の責任のもと、すべてネットワーク機器や管理システムを管理していたため、ネットワーク機器の設定、変更、保守に多大な労力が必要であった。

また、ネットワーク構成の変更や新しい不正侵入の手法に対応するための新規導入およびバージョンアップのコストも大きく、迅速に対応できていなかった。

例えば、特開２０００－４７９８７や特開平６－６３４７では、不正アクセス検出後の対処方法は管理者の采配に委ねられており、特開２０００－４７９８７では、擬似データベースへ侵入者を誘導する対策が取られているものの、ネットワークを運営している組織で擬似データベースの設置を行わなければならない。

【０００４】

この発明は、上記のような問題点を解決するためになされたもので、ネットワーク利用者もしくは管理者に代わって、不正侵入の防御や対処を行う集中管理システムを提供することを目的とする。

【０００５】

このような集中管理システムを利用するサービス利用者側は、おとりサーバ（擬似サーバ）の設置やログ解析、応答パケットの作成といった対処を専門のサービス業者に委託することによって、ネットワーク管理のコストを軽減することができるという利点がある。

また、サービス提供者側は、サービス利用者のネットワーク機器の状況を遠隔地から常時把握することができるため、サービス利用者のところに、出向かずとも迅速な対応が可能となる。

【０００６】

【課題を解決するための手段】

本発明に係る不正侵入データ対策処理装置は、

所定の内部通信ネットワーク外に配置され、

前記内部通信ネットワークに不正に侵入する目的で前記内部通信ネットワーク外に配置されたいずれかのデータ通信装置より送信された不正侵入データを受信し、受信した前記不正侵入データに対する対策処理を行うことを特徴とする。

【０００７】

前記不正侵入データ対策処理装置は、

前記内部通信ネットワーク内に配置されたデータ通信装置と前記内部通信ネットワーク外に配置されたデータ通信装置との間のデータ通信の中継を行うととと

もに前記不正侵入データを検知する不正侵入データ検知装置に接続され、

前記不正侵入データ検知装置より前記不正侵入データを受信することを特徴とする。

【０００８】

前記不正侵入データ対策処理装置は、

前記不正侵入データ検知装置より、前記不正侵入データを受信するデータ受信部と、

前記データ受信部により受信された前記不正侵入データを解析するデータ解析部と、

前記データ解析部による解析結果に基づき、前記不正侵入データに対する応答データを生成する応答データ生成部と、

前記応答データ生成部により生成された前記応答データを前記不正侵入データ検知装置に対して送信するデータ送信部とを有することを特徴とする。

【０００９】

前記データ受信部は、

前記不正侵入データ検知装置より、前記不正侵入データ検知装置によりカプセル処理された不正侵入データを受信し、

前記不正侵入データ対策処理装置は、更に、

前記データ受信部により受信されたカプセル処理された不正侵入データのカプセル処理を解除して不正侵入データを抽出するとともに、前記応答データに対してカプセル処理を行うカプセル処理部を有し、

前記データ送信部は、

前記カプセル処理部によりカプセル処理された応答データを前記不正侵入データ検知装置に対して送信することを特徴とする。

【００１０】

前記応答データ生成部は、

前記内部通信ネットワーク内に配置された特定のデータ通信装置が前記不正侵入データを受信した場合に、前記特定のデータ通信装置が前記不正侵入データに対して生成する応答データと同じ内容の応答データを生成することを特徴とする

【００１１】

前記データ受信部は、

前記不正侵入データ検知装置より、前記不正侵入データ検知装置の通信履歴を示す通信履歴情報を受信し、

前記データ解析部は、

前記データ受信部により受信された前記通信履歴情報を解析し、前記通信履歴情報の解析結果に基づき前記内部通信ネットワーク外に配置された所定のデータ通信装置から送信されるデータを不正侵入データに指定する不正侵入データ指定情報を生成し、

前記データ送信部は、

前記データ解析部により生成された前記不正侵入データ指定情報を前記不正侵入データ検知装置に送信することを特徴とする。

【００１２】

前記データ受信部は、

前記不正侵入データ検知装置より、データ認証に用いる認証情報が添付された不正侵入データを受信し、

前記カプセル処理部は、前記認証情報を用いて前記不正侵入データのデータ認証を行うことを特徴とする。

【００１３】

前記カプセル処理部は、

前記応答データのデータ認証に用いる認証情報を前記応答データに添付し、

前記データ送信部は、

前記カプセル処理部により認証情報が添付された応答データを前記不正侵入データ検知装置に送信することを特徴とする。

【００１４】

本発明に係る不正侵入データ対策処理方法は、

所定の内部通信ネットワーク外において、

前記内部通信ネットワークに不正に侵入する目的で前記内部通信ネットワーク

外に配置されたいずれかのデータ通信装置より送信された不正侵入データを受信し、受信した前記不正侵入データに対する対策処理を行うことを特徴とする。

【００１５】

前記不正侵入データ対策処理方法は、

前記内部通信ネットワーク内に配置されたデータ通信装置と前記内部通信ネットワーク外に配置されたデータ通信装置との間のデータ通信の中継を行うとともに前記不正侵入データを検知する不正侵入データ検知装置と通信を行い、

前記不正侵入データ検知装置より前記不正侵入データを受信することを特徴とする。

【００１６】

前記不正侵入データ対策処理方法は、

前記不正侵入データ検知装置より、前記不正侵入データを受信するデータ受信ステップと、

前記データ受信ステップにより受信された前記不正侵入データを解析するデータ解析ステップと、

前記データ解析ステップによる解析結果に基づき、前記不正侵入データに対する応答データを生成する応答データ生成ステップと、

前記応答データ生成ステップにより生成された前記応答データを前記不正侵入データ検知装置に対して送信するデータ送信ステップとを有することを特徴とする。

【００１７】

前記応答データ生成ステップは、

前記内部通信ネットワーク内に配置された特定のデータ通信装置が前記不正侵入データを受信した場合に、前記特定のデータ通信装置が前記不正侵入データに対して生成する応答データと同じ内容の応答データを生成することを特徴とする。

【発明の実施の形態】

実施の形態１．

図１は、この発明に係る不正侵入データ対策処理装置を含むネットワークシス

テムの全体構成図である。

図１において、１は不正侵入対策サービスを実施する管理代行業者のデータセンタであり、１１はデータセンタ内に設置された管理システム、１２は、顧客情報を格納する顧客データベース、１３は、不正侵入者を誘導し、情報を取得するためのおとりサーバ、１４は、不正侵入情報を解析する際に用いられる知識ベースである。

２はインターネット、３は不正侵入対策サービスのサービス契約者が使用しているネットワーク機器、４はサービス契約者が使用する一般端末、５はサービス契約者が保持している不正侵入者の攻撃対象となる攻撃対象サーバ、６は不正侵入者の端末である。

ここで、管理システム１１及びおとりサーバ１３は、不正侵入データ対策処理装置として機能し、ネットワーク機器３は、不正侵入データ検知装置として機能する。

また、ネットワーク機器３、一般端末４、攻撃対象サーバ５は、同一の内部通信ネットワークに属する。

【００１８】

また、図２は、ネットワーク機器３の機能ブロック図を示している。

ネットワーク機器３は、データの受信および送信を行うデータ収集／送出部３１と、一般的な通信か管理システム１１からのおとりサーバへの誘導パケット（応答パケット）かを判別する識別情報判別部３２と、不正侵入パケットを検出する不正侵入検出部３３と、不正侵入パケットもしくはログデータを管理システム１１に転送するためにエンカプセル処理を施したり、管理システム１１から送られた応答パケットのデカプセル処理を行うパケットカプセル処理部３４と、ネットワーク機器３を通過したデータを記録するログ取得部３５から構成されている。

【００１９】

また、図３は、管理システムの機能ブロック図を示している。

管理システム１１は、データの受信および送信を行うデータ受信／送信部１１１、受信したパケットが契約者からのものかを照会する顧客照会部１１２、ネッ

トワーク機器３から入手したデータの種別を判別するデータ種別判別部１１３、ネットワーク機器３から転送された、エンカプセルされた侵入パケットもしくはログデータのデカプセル処理とネットワーク機器３へ送信する応答パケット（応答データ）のエンカプセル処理を行うパケットカプセル処理部１１４、入手したログデータおよび侵入パケットを解析する不正データ解析部１１５から構成される。

また、データセンタ１には、この他、管理システム１１と情報をやりとりする顧客データベース１２、おとりサーバ１３、知識ベース１４がある。

なお、おとりサーバ１３は、不正侵入パケットに対する応答データ（応答パケット）を生成する応答データ生成部として機能する。

【００２０】

図４にネットワーク機器３、管理システム１１が送受信する通信パケットの構成について示す。

パケットＰ１は、不正侵入パケットである。パケットＰ１は、不正侵入者端末６から送信され、ネットワーク機器３により受信される。

パケットＰ２は、パケットＰ１をエンカプセル化したパケットで、識別情報を含む不正侵入パケットの情報を転送する。パケットＰ２は、ネットワーク機器３から管理システム１１へ送信される。

パケットＰ３は、エンカプセル化された応答パケットで、識別情報を含む不正侵入者に対する応答パケット情報を転送する。パケットＰ３は、管理システム１１からネットワーク機器３へ送信される。

パケットＰ４は、パケットＰ３をデカプセル化したパケットで、攻撃対象サーバ５からの応答を模擬したおとりサーバ１３からの応答パケットである。パケットＰ４には、攻撃対象サーバ５が応答する内容と同じ情報が格納されており、本来そのままではインターネット上には送出できないが、パケットＰ３に示すようにエンカプセル化することによってネットワーク機器３への転送を可能にしている。

【００２１】

次にネットワークシステム全体の動きについて説明する。

図５は、不正侵入者が内部通信ネットワークに不正侵入した場合の対策処理の流れを示す。

まず、ある不正侵入者端末６がある契約者のネットワーク（内部通信ネットワーク）内に設置されたサーバ（攻撃対象サーバ）５に不正侵入しようして、不正侵入パケットＰ１を送信したとする（ステップ１０１）。

これに対して、ネットワーク機器３において、不正侵入パケットＰ１を検出する。不正侵入パケットＰ１を検出したネットワーク機器３は、不正侵入パケットＰ１（侵入パケット情報）をエンカプセル化してパケットＰ２を生成し、パケットＰ２をデータセンタ１に転送する（ステップ１０２）。これによりネットワーク機器３は、不正侵入パケットＰ１による攻撃対象サーバ５への不正侵入を防ぐことができる。

次に、データセンタ１の管理システム１１では、ネットワーク機器３からパケットＰ２を受信し、受信したパケットＰ２を解析し、攻撃対象サーバ５からの応答に見せかけた、おとりサーバ１３からの応答パケットＰ４をエンカプセル化してパケットＰ３を生成し、パケットＰ３をネットワーク機器３に送り返す（ステップ１０３）。

次に、ネットワーク機器３は、管理システム１１よりパケットＰ３を受信し、受信したパケットＰ３をデカプセル化して応答パケットＰ４を取りだし、不正侵入者端末６に対して応答パケットＰ４を送信する（ステップ１０４）。不正侵入者は、応答パケットＰ４を攻撃対象サーバ５からの応答だと思い込み、おとりサーバ１３に侵入を開始する。

不正侵入者端末６とおとりサーバ１３との交信は、毎回ステップ１０１～ステップ１０４の手順により行なわれる。おとりサーバ１３でのログ解析により不正侵入のより詳細な手口が明らかになる。

【００２２】

次にネットワーク機器３の動作について説明する。

図６に、ネットワーク機器３における通信パケットの処理についてフローチャートを示す。

まず、ネットワーク機器３はデータ収集／送出部３１より、通信パケットを受

信すると（ステップ３０１）、識別情報判別部３２で、そのパケットが管理システム１１からのエンカプセル化された応答パケットＰ３なのか、単なる中継パケットなのかを受信パケットの識別情報により判別する（ステップ３０２）。

この結果、エンカプセル化された応答パケットＰ３である場合、パケットカプセル処理部３４で、エンカプセル化された応答パケットＰ３のデカプセル処理を行い（ステップ３０３）、不正侵入者端末６への応答パケットＰ４として不正侵入者端末６に送信する（ステップ３０６）。

一方、単なる中継パケットである場合、不正侵入検出部３３で、不正侵入パケットＰ１かどうかのチェックを行う（ステップ３０４）。ここで、不正侵入パケットＰ１であると判断された場合は、不正侵入パケットＰ１を管理システム１１に転送するため、パケットカプセル処理部３４で不正侵入パケットＰ１をエンカプセルしてパケットＰ２とし（ステップ３０５）、エンカプセル化した不正侵入パケットＰ２をデータ収集／送出部３１から管理システム１１に送信する（ステップ３０６）。

ステップ３０４の不正侵入チェックにより、正常パケットと判断された場合は、そのままデータ収集／送出部３１から送信先にパケットを中継する（ステップ３０６）。

【００２３】

次に管理システム１１の動作について説明する。

図７に、管理システム１１における契約者のネットワーク機器３からの受信パケットに対する処理の流れを示す。

まず、管理システム１１は、データ受信／送信部１１１より、通信パケットを受信すると顧客照会部１１２で顧客データベース１２を参照し、契約者からのパケットであるかどうかを照合する。この照合に成功しなかったパケットは、不正データとして廃棄するか、管理システムの別タスクで処理する（本発明の範囲外）。

受信パケットの照合に成功した場合、データ種別判別部１１３により、ネットワーク機器３から送信されたパケットのデータが不正侵入パケットを転送したもの（パケットＰ２）であるか否かを判別する。

次に、受信したパケットＰ２は、ネットワーク機器３によってエンカプセルされているため、このパケットＰ２をパケットカプセル処理部１１４で、デカプセル処理する。

【００２４】

次に、パケットカプセル処理部１１４でデカプセル処理された不正侵入パケットＰ１は、不正データ解析部１１５に渡され、不正データ解析部１１５は、知識ベース１４を参照しながら、抽出された不正侵入パケットＰ１の解析を行う。知識ベース１４には、この解析結果が反映され、今後の解析のための参考事例として追加される。不正データ解析部１１５は、解析結果をおとりサーバ１３に通知し、おとりサーバ１３から応答パケットＰ４を受け取る。応答パケットＰ４は、不正侵入パケットＰ１が、攻撃対象サーバ５に受信されたとした場合に、不正侵入パケットに対する攻撃対象サーバ５からの応答と同様の情報を有するパケットである。

この応答パケットＰ４を攻撃対象サーバ５からネットワーク機器３経由で送信されたパケットに見せかけるため、パケットカプセル処理部１１４でエンカプセルしてパケットＰ３とした後、データ受信／送信部１１１からネットワーク機器３に対してパケットＰ３を送信する。

この後、ネットワーク機器３では、前述したように、パケットＰ３をデカプセル処理して、応答パケットＰ４を抽出し、抽出した応答パケットＰ４を不正侵入者端末６へ送信する。

【００２５】

以上のように、ネットワーク機器３で検出した不正侵入パケットをネットワーク機器３自身で対処するのではなく、管理システム１１に転送することによって応答パケットを獲得し、不正侵入者を代行業者のデータセンタ内に設置されたおとりサーバに誘導するようにしているので、顧客のネットワークとは独立した侵入対処サービスを実現することができる。

【００２６】

実施の形態２．

以上の実施の形態１では、不正侵入者端末からの不正侵入パケットをネットワ

ーク機器３からデータセンタ１へ転送するようにしたものであるが、次に、不正侵入パケットの早期発見のためネットワーク機器３のログ情報をデータセンタ１へ転送する実施の形態を示す。

図８は、このような場合のネットワークシステム全体の動きを示したものである。

【００２７】

図において、ステップ１０１～ステップ１０４は、実施の形態１において説明したものと同様であり、本実施の形態においては、ステップ１０５及びステップ１０６について説明する。

ネットワーク機器３は、ログ取得部３５（図２）により、常に外部からアクセス情報を記録している。このログ情報（通信履歴情報）をエンカプセル化し、管理システム１１からの命令もしくはネットワーク機器３自身の定期的なトリガにより管理システム１１にパケットＰ５として転送する（ステップ１０５）。

ここで、パケットＰ５の構成を図９に示す。パケットＰ５は、ログ情報をエンカプセル化したパケットで、ネットワーク機器のログ情報を管理システムに転送するパケットである。。

次に、管理システム１１では、パケットカプセル処理部１１４がパケットＰ５をデカプセル化し、不正データ解析部１１５がログ情報を解析する。ここで、問題のあった場合、即ち、不正侵入パケットの疑いのあるパケットが発見された場合は、ネットワーク機器３における不正侵入検出部３３の設定情報を更新するため、管理システム１１は新しい侵入検出設定情報をネットワーク機器３に送信する（ステップ１０６）。ここで、侵入検出設定情報とは、ネットワーク機器３に対して不正侵入パケットの疑いがあるパケットを通知し、不正侵入パケットの疑いのあるパケットを送信した端末より以後送信されたパケットを不正侵入パケットとして取り扱うようにネットワーク機器３に対して指示する情報である。即ち、侵入検出設定情報は、不正侵入データ指定情報に相当する。また、侵入検出設定情報は、不正データ解析部１１５により生成される。

以降、不正侵入の疑いのある送信元からのアクセスは、ネットワーク機器３の不正侵入検出部３３にて不正侵入パケットと判断される。例えば、端末６からの

アクセスログを管理システム１１が不正と判断した場合、端末６からのアクセスを拒否する設定情報をネットワーク機器３に送信する。この結果、ネットワーク機器３は、端末６からのアクセス（ステップ１０１）を不正侵入パケットとして検出し、端末６からのパケット（Ｐ１：不正侵入パケット）をエンカプセル化した後（Ｐ２）、管理システム１１に転送する（ステップ１０２）。以降の処理手段は、実施の形態１と同様である。

【００２８】

本形態に関するネットワーク機器３および管理システム１１の振舞いは、実施の形態１にほぼ等しい。

ただし、管理システム１１において、図６に示すデータ種別判別部１１３は、受信データに含まれる識別情報から、ネットワーク機器３からの受信パケットがエンカプセル化された不正侵入パケットＰ２ではなく、ログ情報パケットＰ５であることを判別する。そして、不正データ解析部１１５において、ログ情報パケットＰ５の解析を行う。

また、管理システム１１では、不正データ解析部１１５は、不正侵入パケットの疑いがあるパケットを発見した場合、新しい侵入設定検出情報を生成し、データ受信／送信部１１１は、生成された新しい侵入設定検出情報をネットワーク機器３に送信する。

【００２９】

以上のように、ネットワーク機器３のログ情報を管理システム１１に転送することによって集中的な解析を依頼し、その結果、応答パケットを獲得し、不正侵入者を代行業者のデータセンタ内に設置されたおとりサーバに誘導するようにしているので、顧客のネットワークとは独立した侵入対処サービスを実現することができる他、直接の攻撃ではなくとも不正侵入のおそれのあるパケットの侵入を防止することにより、不正侵入の早期発見につながる。

【００３０】

実施の形態３．

以上の実施の形態１および２では、転送するパケットをエンカプセル化し、識別情報により、転送するデータ内容を判別している。

次に、本実施の形態において、管理システム１１およびネットワーク機器３にて送受信するパケットに認証情報を付加する場合について示す。

【００３１】

図１０において、パケットＰ２を例に認証情報を付加したパケットＰ２Ｈを示す。

パケットＰ２Ｈでは、識別情報以降のデータを入力値とするハッシュ等の認証情報を識別情報の前に付加している。

ネットワーク機器３における認証情報の付加および認証情報チェックは、パケットカプセル処理部３４のエンカプセル／デカプセル処理で行う。管理システム１１における認証情報の付加および認証情報チェックは、パケットカプセル処理部１１４のエンカプセル／デカプセル処理で行う。

なお、上記の例では、パケットＰ２に認証情報が付加されたパケットＰ２Ｈを説明したが、同様な構成によりパケットＰ３に認証情報が付加されたパケットＰ３Ｈの送受信も行うことができる。

【００３２】

以上のように、通信パケットに認証情報を追加することによって、管理システムとネットワーク機器との間の通信のセキュリティを向上させる効果がある。

【００３３】

なお、以上の実施の形態１～実施の形態３では、本発明に係る不正侵入データ対策処理装置について説明してきたが、同様の処理手順により本発明に係る不正侵入データ対策処理方法を実現することもできる。

【００３４】

ここで、以上にて説明してきた本発明の特徴を示すと以下のようになる。

本発明は、コンピュータネットワークシステムにおける不正侵入対策に関して、サポート契約者のネットワークセキュリティ集中管理サービスを提供する。

集中管理サービスの一つとして、不正侵入者をサポート提供者のおとりサーバに誘導する。

サービス利用者のネットワーク機器は、不正侵入を検出すると、不正侵入パケットをサービス提供者のデータセンタ内の管理システムに制御情報を施し（エン

カプセル処理）、転送する。データセンタには、管理システム、擬似サーバ（ここではおとりサーバと呼ぶ）等が設置されている。おとりサーバは、不正侵入者の標的となっていたサービス利用者の攻撃対象サーバに見せかけて誘導するためのもので、攻撃対象サーバと同じ応答を返す。管理システムでは、転送された不正侵入パケットの制御情報を解いて（デカプセル処理）解析する。また、おとりサーバからの応答をエンカプセルし、ネットワーク機器に転送する。

管理システムからの応答パケットを受信したネットワーク機器は、応答パケットをデカプセルし、送出する。不正侵入者はこの応答パケットを攻撃対象サーバとの応答だと思い込むが、ネットワーク機器を介して、データセンタのおとりサーバとやりとりしていることとなり、おとりサーバに誘導される。

【００３５】

本発明は、コンピュータネットワークシステムにおける不正侵入対策に関して、サポート契約者のネットワークセキュリティ集中管理サービスを提供する。

集中管理サービスの一つとして、不正侵入者をサポート提供者のおとりサーバに誘導する。

サービス利用者のネットワーク機器は、定期的にログ情報をエンカプセル化して、サービス提供者に転送する。データセンタの管理システムでは、ログ情報を解析し、不正が認められた場合、管理システムからの通知によりネットワーク機器の不正侵入検出の設定情報を更新することを特徴とする。

【００３６】

本発明は、集中管理サービスが送受信するパケットに関して、認証情報の負荷または暗号化により、セキュリティ強度を向上させることを特徴とする。

【００３７】

【発明の効果】

本発明によれば、ネットワーク機器で検出した不正侵入パケットをネットワーク機器自身で対処するのではなく、管理システムに転送することによって応答パケットを獲得し、不正侵入者を代行業者のデータセンタ内に設置されたおとりサーバに誘導するようにしているので、顧客のネットワークとは独立した侵入対処サービスを実現することができる。

【００３８】

また、本発明によれば、直接の攻撃ではなくとも不正侵入のおそれのあるパケットの侵入を防止することにより、不正侵入に対する有効な対策を行うことができる。

【００３９】

また、本発明によれば、通信パケットに認証情報を追加することによって、管理システムとネットワーク機器との間の通信のセキュリティを向上させる効果がある。

【図面の簡単な説明】

【図１】　ネットワークシステムの全体構成を示す図。

【図２】　ネットワーク機器の機能ブロックを示す図。

【図３】　データセンタの機能ブロックを示す図。

【図４】　通信パケットＰ１～Ｐ４の構成を示す図。

【図５】　実施の形態１における不正侵入パケット対策処理の手順を示す図。

【図６】　ネットワーク機器の処理フローを示す図。

【図７】　データセンタの処理フローを示す図。

【図８】　実施の形態２における不正侵入パケット対策処理の手順を示す図。

【図９】　通信パケットＰ５の構成を示す図。

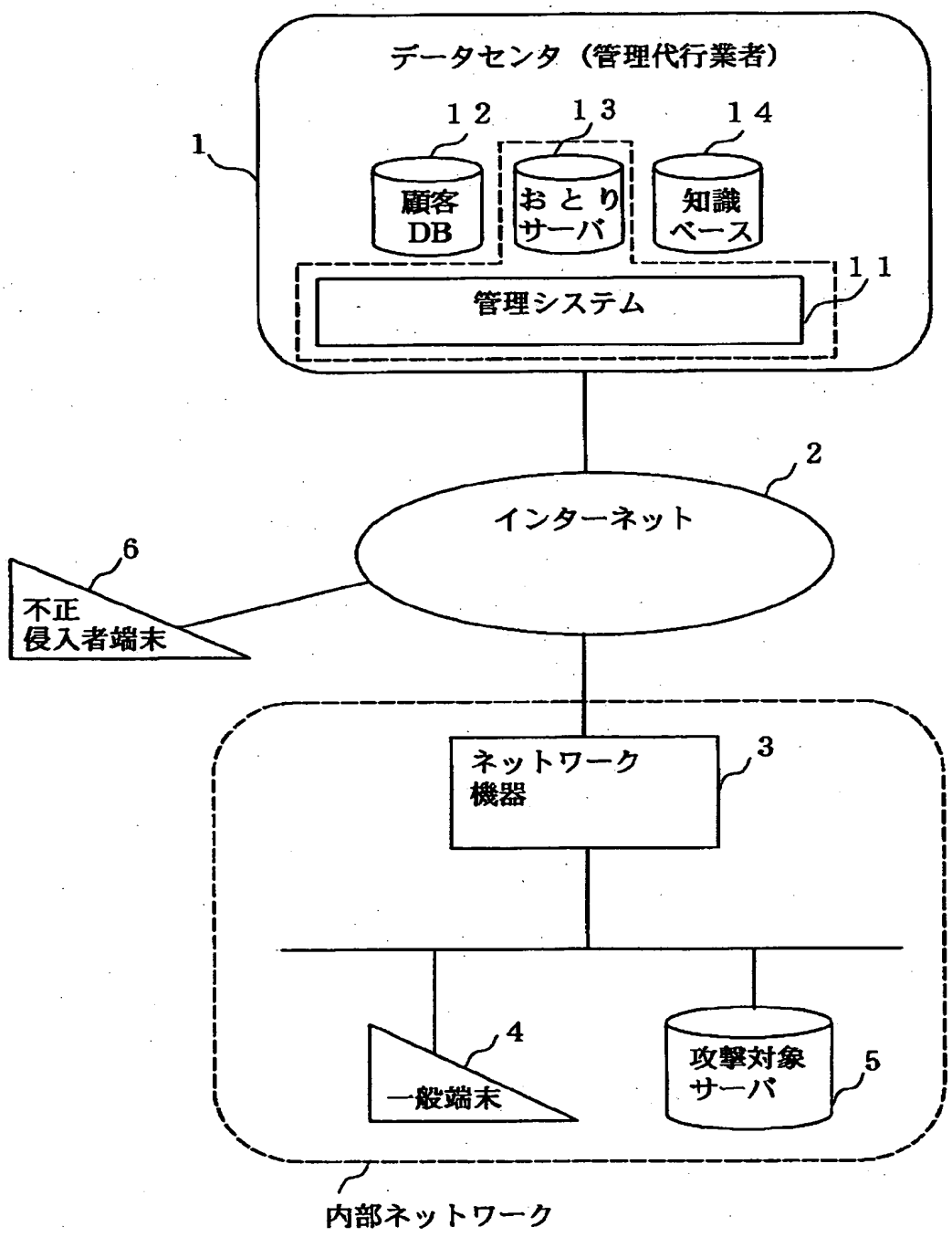
【図１０】　通信パケットＰ２Ｈの構成を示す図。

【符号の説明】

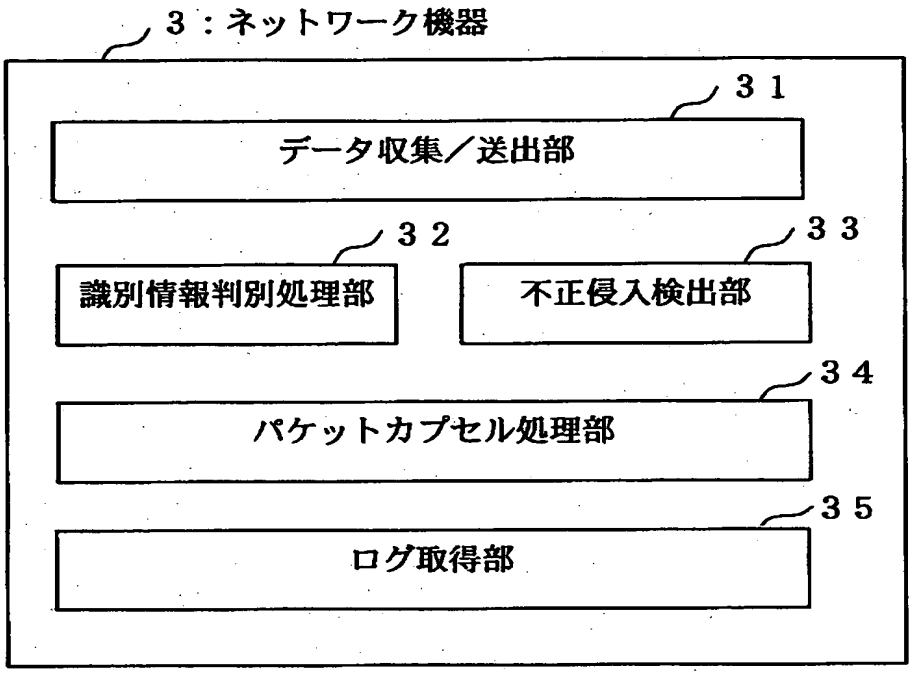
１　データセンタ、２　インターネット、３　ネットワーク機器、４　一般端末、５　攻撃対象サーバ、６　不正侵入者端末、１１　管理システム、１２　顧客データベース、１３　おとりサーバ、１４　知識ベース。

【書類名】　　図面

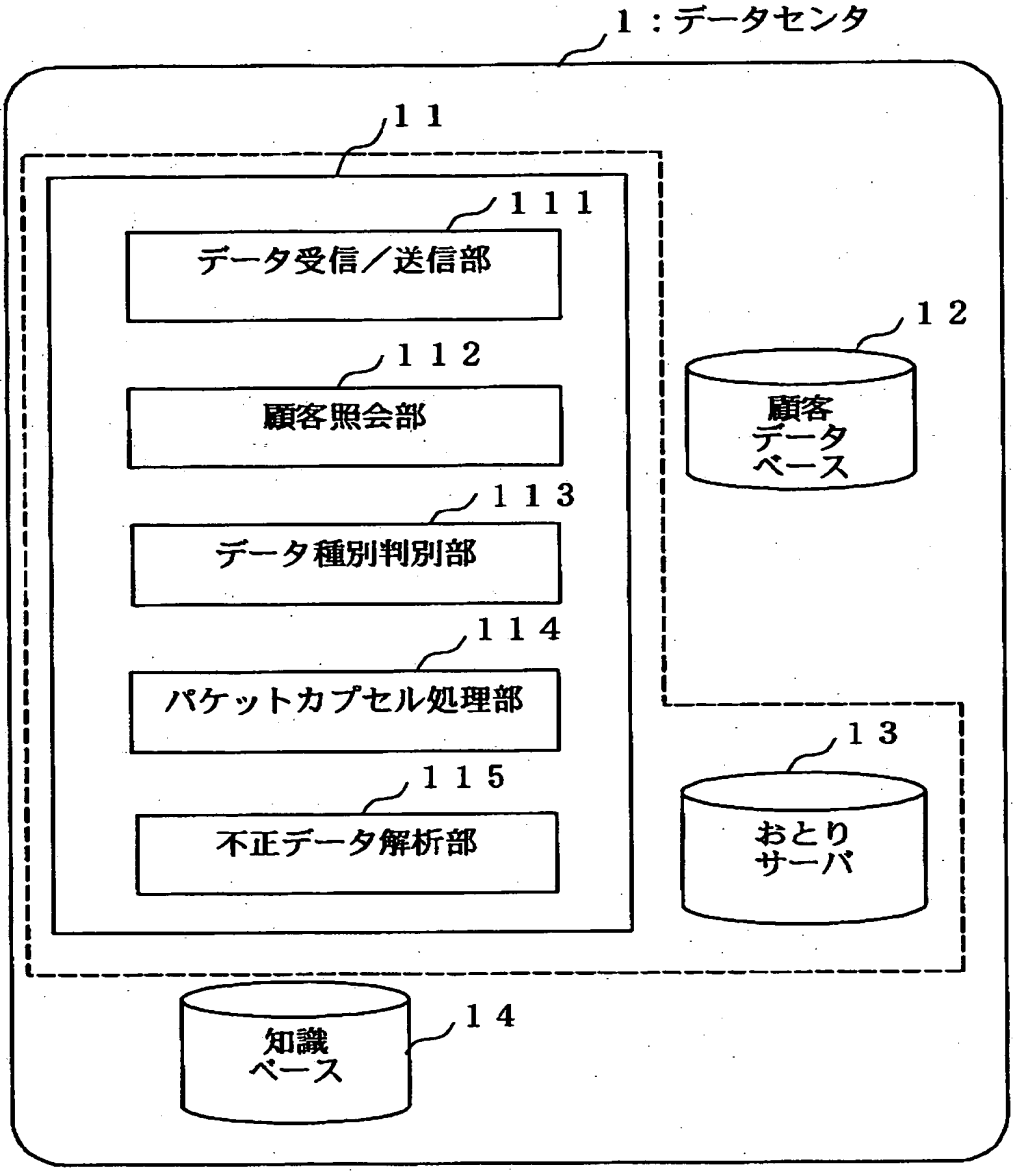
【図１】


データセンタ（管理代行業者）
1
12
13
14
顧客
DB
おとり
サーバ
知識
ベース
11
管理システム
2
インターネット
6
不正
侵入者端末
ネットワーク
機器
3
4
一般端末
攻撃対象
サーバ
5
内部ネットワーク

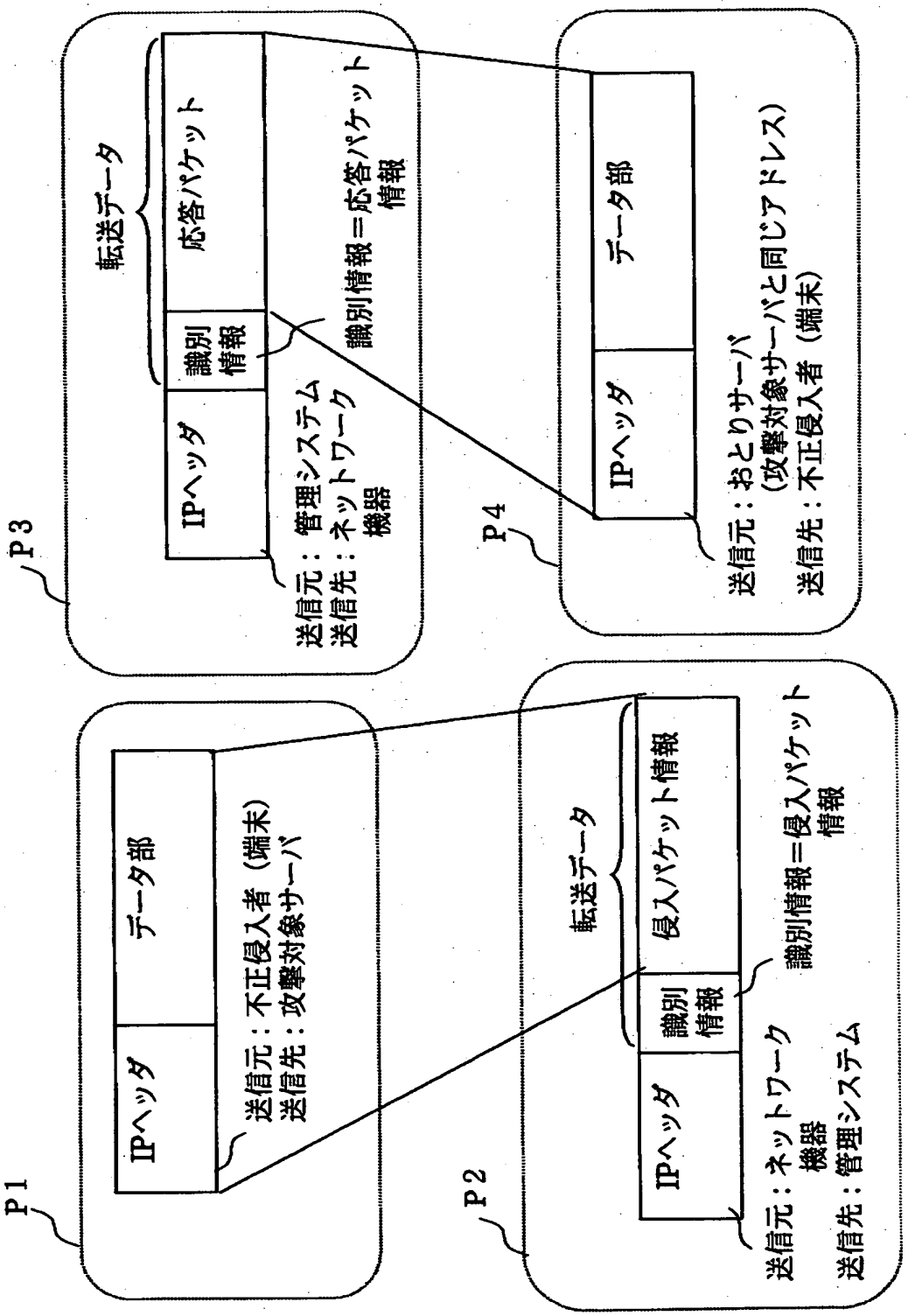
【図２】


３：ネットワーク機器
３１
データ収集／送出部
３２
識別情報判別処理部
３３
不正侵入検出部
３４
パケットカプセル処理部
３５
ログ取得部

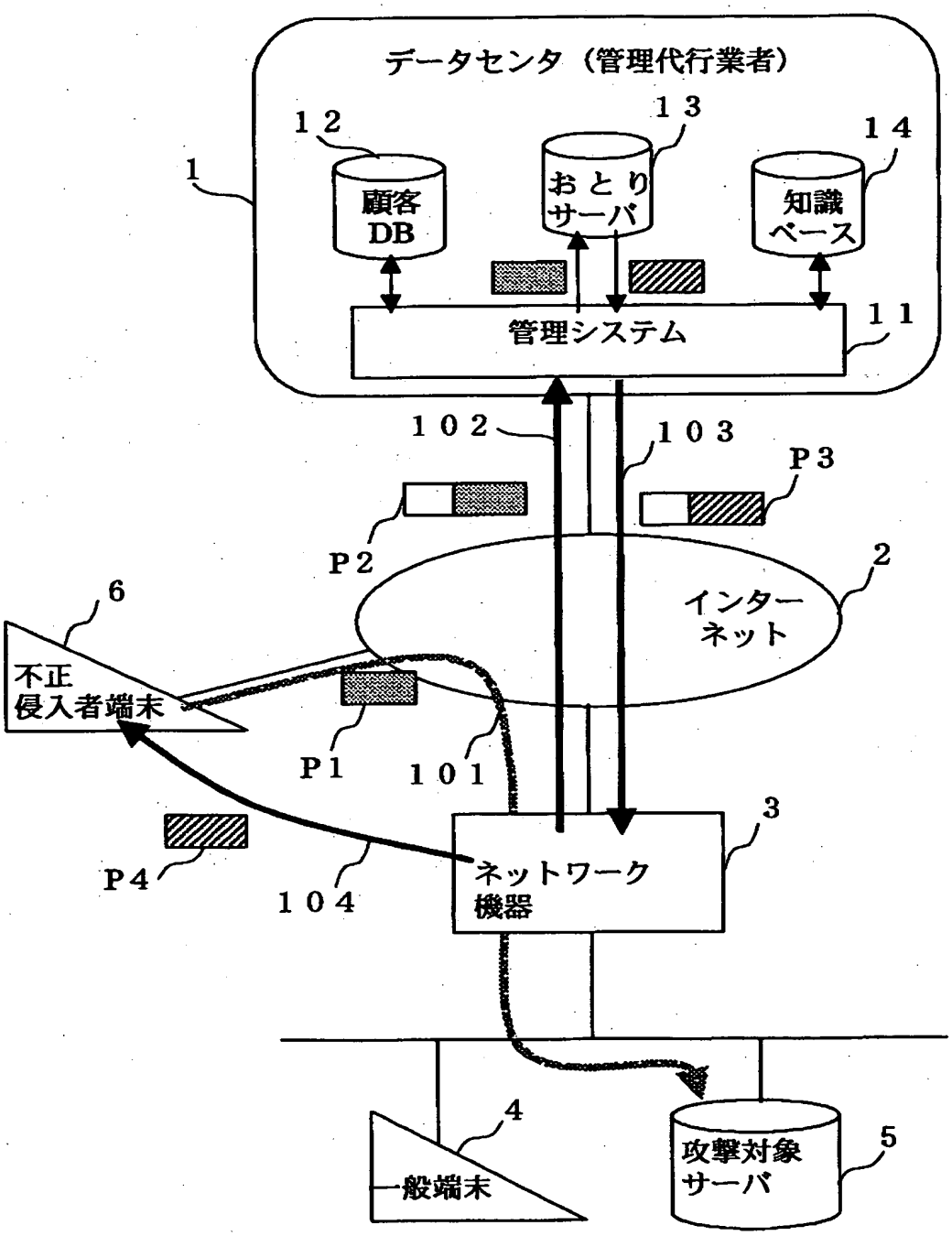
【図３】


１：データセンタ
１１
１１１
データ受信／送信部
１１２
顧客照会部
１１３
データ種別判別部
１１４
パケットカプセル処理部
１１５
不正データ解析部
１２
顧客
データ
ベース
１３
おとり
サーバ
１４
知識
ベース

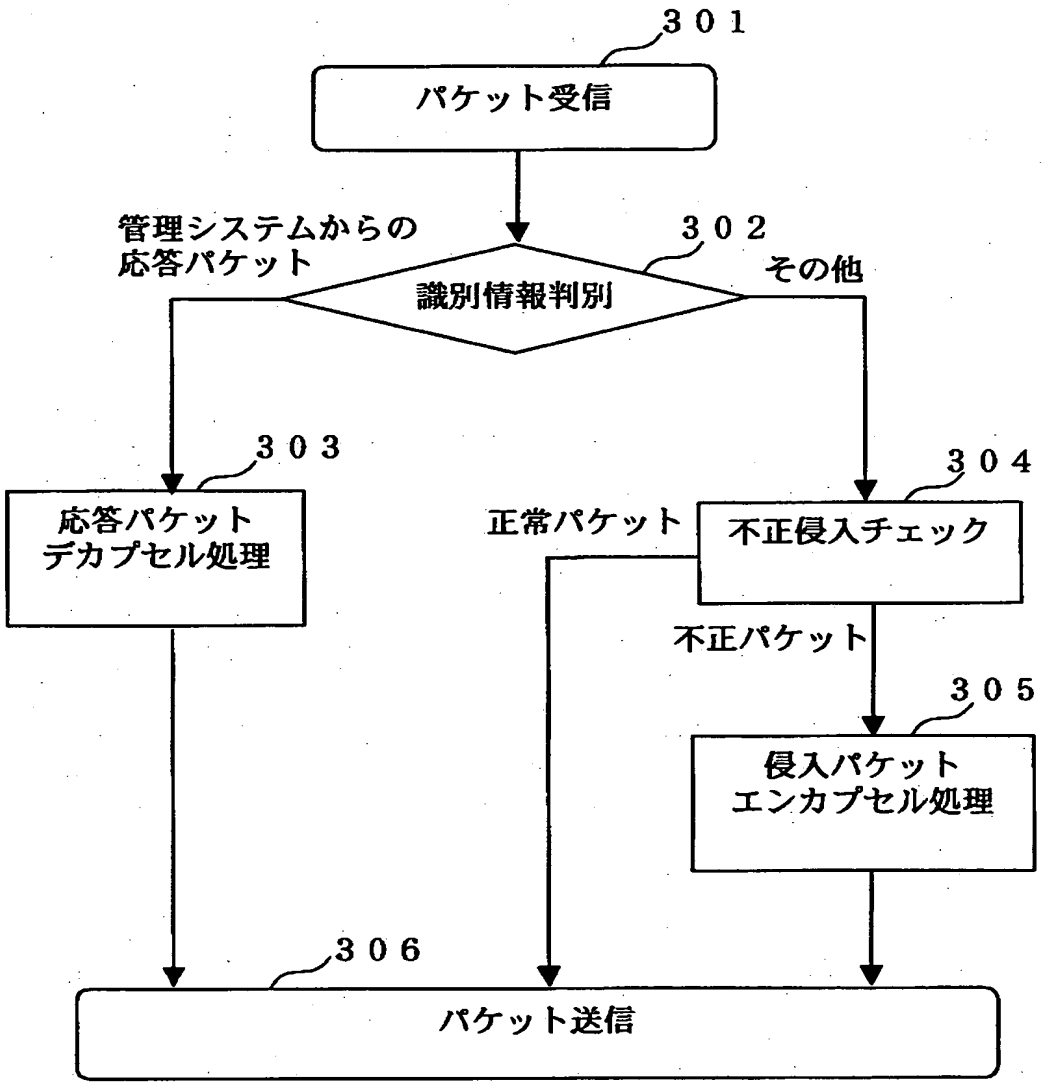
【図４】


P1
IPヘッダ
データ部
送信元：不正侵入者（端末）
送信先：攻撃対象サーバ
P2
転送データ
IPヘッダ
識別情報
侵入パケット情報
送信元：ネットワーク機器
送信先：管理システム
識別情報＝侵入パケット情報
P3
転送データ
IPヘッダ
識別情報
応答パケット
送信元：管理システム
送信先：ネットワーク機器
識別情報＝応答パケット情報
P4
IPヘッダ
データ部
送信元：おとりサーバ
（攻撃対象サーバと同じアドレス）
送信先：不正侵入者（端末）

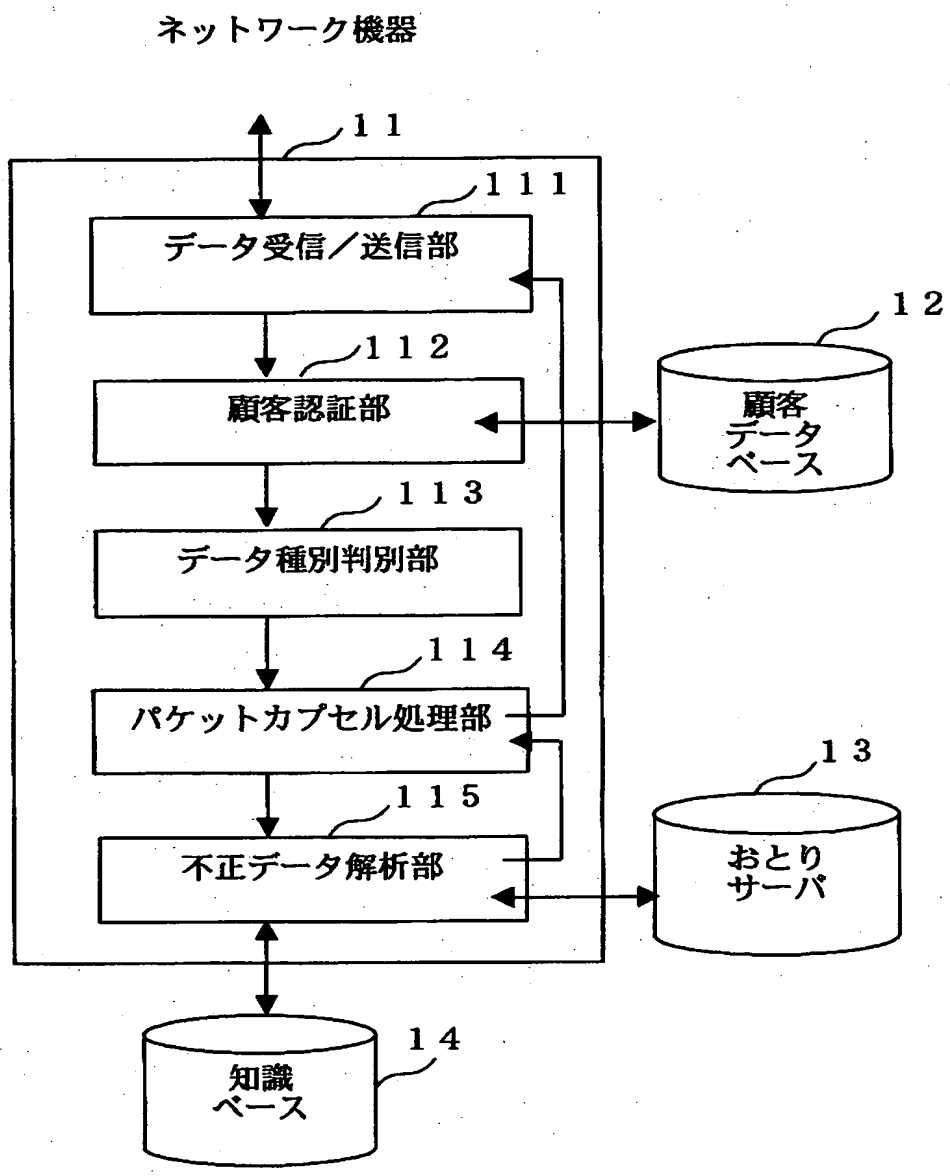
【図５】


データセンタ（管理代行業者）
１２
１３
１４
１
顧客
DB
おとり
サーバ
知識
ベース
管理システム
１１
１０２
１０３
P３
P２
２
インター
ネット
６
不正
侵入者端末
P１
１０１
３
P４
１０４
ネットワーク
機器
４
攻撃対象
サーバ
５
一般端末

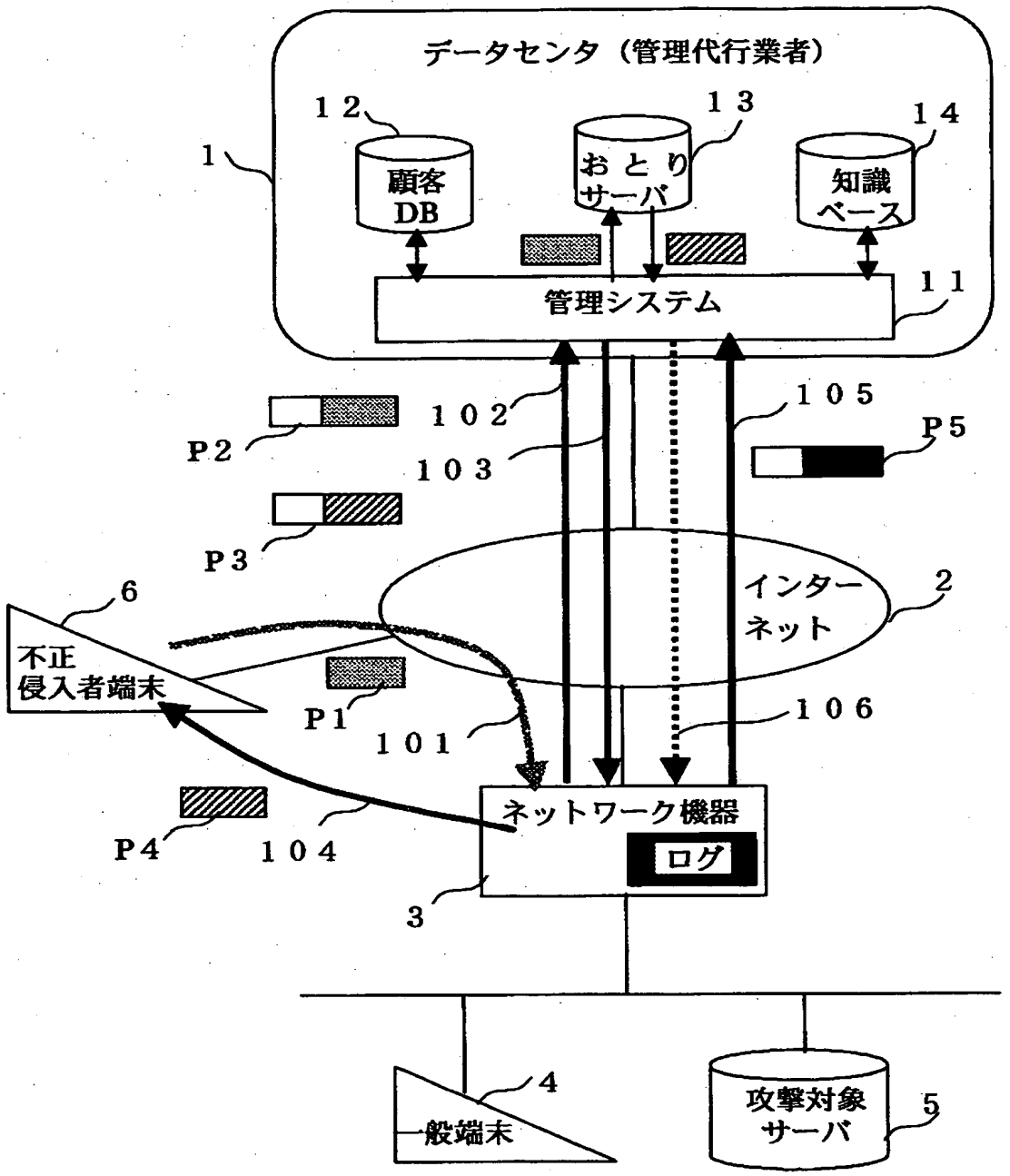
【図６】


３０１
パケット受信
管理システムからの
応答パケット
３０２
識別情報判別
その他
３０３
応答パケット
デカプセル処理
３０４
正常パケット
不正侵入チェック
不正パケット
３０５
侵入パケット
エンカプセル処理
３０６
パケット送信

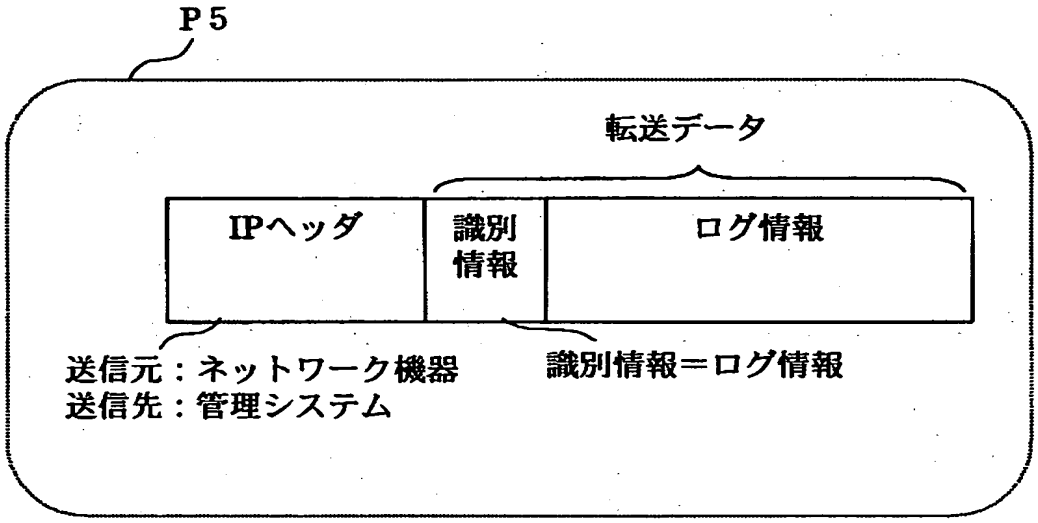
【図７】


ネットワーク機器
１１
１１１
データ受信／送信部
１１２
顧客認証部
１１３
データ種別判別部
１１４
パケットカプセル処理部
１１５
不正データ解析部
１２
顧客
データ
ベース
１３
おとり
サーバ
１４
知識
ベース

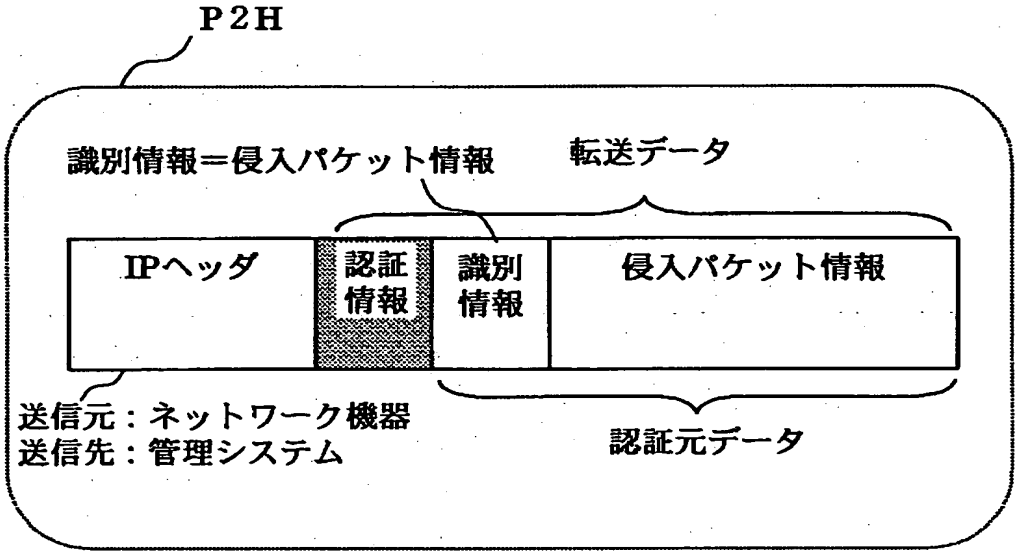
【図８】


データセンタ（管理代行業者）
１２
１３
１４
１
顧客
DB
おとり
サーバ
知識
ベース
管理システム
１１
１０２
１０５
P５
P２
１０３
P３
インター
ネット
２
６
不正
侵入者端末
P１
１０１
１０６
ネットワーク機器
ログ
P４
１０４
３
４
一般端末
攻撃対象
サーバ
５

【図９】



【図１０】


P2H
識別情報＝侵入パケット情報
転送データ
IPヘッダ
認証情報
識別情報
侵入パケット情報
送信元：ネットワーク機器
送信先：管理システム
認証元データ

【書類名】　　要約書

【要約】

【課題】　不正侵入の防御や対処を行う集中管理システムを提供する。

【解決手段】　ネットワーク機器３は、不正侵入者端末６から送信された不正侵入パケットＰ１を検出し、不正侵入パケットＰ１をエンカプセル化したパケットＰ２をデータセンタ１に転送し、データセンタ１の管理システム１１は、パケットＰ２を解析し、攻撃対象サーバ５からの応答に見せかけた、おとりサーバ１３からの応答パケットＰ４をエンカプセル化してパケットＰ３とし、パケットＰ３をネットワーク機器３に送信し、ネットワーク機器３は、パケットＰ３をデカプセル化して応答パケットＰ４を取りだして不正侵入者端末６に送信し、これにより不正侵入者端末６は、応答パケットＰ４を攻撃対象サーバ５からの応答と思い込み、おとりサーバ１３に侵入を開始する。

【選択図】　　図５

出　願　人　履　歴　情　報

識別番号　　〔０００００６０１３〕

１．変更年月日　　１９９０年　８月２４日
［変更理由］　新規登録
住　所　　東京都千代田区丸の内２丁目２番３号
氏　名　　三菱電機株式会社